GSA FPMR (41 CFR) 101-11.6

UNITED STATES GOVERNMENT

Memorandum

TO : S46

STATU : R1

DATE: 16 JUL 1975

FROM : R14

SUBJECT: Computer Security Monitoring

1. Reference: S46 memorandum, 13 June 1975, subject as above. The reference document has been reviewed by R14 and the following specific comments are provided:

2. The American National Standard Institute (ANSI) definition of monitoring is acceptable as it currently reads.

3. There are documents in existence which prescribe policy and/or guidance for the several facets of ADP security. These documents are not listed in your references. It is not clearly stated in your document whether the paper is a tutorial to educate computer system designers or is intended to be a security monitoring appendix to one of the existing computer security directives.

4. Paragraph three should clearly delineate between those functions of a local security monitor to support a host and its security officer versus functions to support a network control center and network security officer. The working paper does not address monitoring of the communications subsystem of a computer network.

5. There appears to be duplication of function between the security monitor and the access controller for a particular host. The functions of each of these subsystems should be delineated.

6. When recording "actions" requested by a user in paragraphs 3.1c and 3.1d it is not clear what constitutes an "action". What level of detail should the security monitor versus the access controller be concerned with?

7. Paragraph 3.1e appears to place the security monitor squarely in the middle of the host file maintenance operation. The amount of data generated could easily swamp any reasonable security monitoring subsystem.

8. Paragraph 3.1f asks for data on "logical interconnections established within a host." This appears to be and access controller function rather than a security monitor function. It may be reasonable for the security monitor to ocassionally take a snapshot of the host computer to check for consistancy of current accesses with respect to the security profiles for objects and subjects.

9. Obtaining records of hardware and software failure as requested in paragraph 3.1g may be difficult to do in real time. Even after the fact it is hard to determine the "seriousness" of a system crash caused by an unknown set of hardwire and/or software failures.

10. More explication is needed on the security verification programs referenced in paragraph 3.1h.

11. It is not clear why the Network Control Center would request "increased information flow" from a host security monitoring system as outlined in paragraph 3.1j.

12. Omitted from paragraph 3.1 is an indication of how the local security monitoring system will support the local ADP system security officer.

13. Paragraph 3.2 does not distinguish between the Network security monitor and the network access controller(s). Also missing is specific monitoring of the communications subsystem.

14. The design requirements in paragraph 3.3a which ask that the security monitor be remote from normal network operations do not address the problems of running and maintaing the monitor subsystems.

STAT

Chief, R14

cc: C43
P13
R1RF
R13
R14
R142(2)
R25
R35
S41
V21

DISTRIBUTION

13 JUN 1975

[redacted] STAT

S46

Computer Security Monitoring

S46 is attempting to define and/or collect requirements/needs for security monitoring in future computers and associated networks. You are invited to provide any comments on the attached draft working paper by 7 July 1975. Any questions should be addressed to [redacted] STAT

[redacted] STAT

[redacted] STAT

Chief, S46

Reference - return to R14

Incl:
S46 Draft Working Paper,
Subj: Security Monitoring,
undtd

DISTRIBUTION:
C309
C42
C43
C44
P13
R13
R14
R25
R35
S03
S12
S13
S35
S41
S42
T41
V21

[redacted] STAT

DRAFT WORKING PAPER

"SECURITY MONITORING"

1. INTRODUCTION

This paper has been written to describe computer security monitoring; that is, what it is, what it should do, and in some cases how it should be implemented. It is hoped that this information will help establish a policy for security monitoring to accommodate the rapid technological advances in computer networks and systems.

2. DEFINITION OF A SECURITY MONITOR

"Monitor" is a term which has many different meanings. According to the American National Standard Institute (ANSI), a monitor is "software or hardware that observes, supervises, controls, or verifies the operations of a system". If the adjective "security" is added to this definition, a problem occurs with the word "control". A security monitor should not control the security operations of a system. Instead it should be transparent to the operations and also the users of the system.

A security monitor will then be defined as software or hardware designed to:

a. Observe security related functions.

b. Check and record the status of the functions.

c. Aid in verifying the integrity of security in a computer system.

3. REQUIREMENTS FOR A SECURITY MONITORING SYSTEM

The following sections describe the requirements for security monitoring

DRAFT WORKING PAPER

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310013-2

at the host and network levels and also some of the requirements for the system design. For this discussion, each section assumes monitoring in a network environment that may use ARPA packet switching technology and may have a structure similar to that shown in Figure 1.

3.1 SECURITY MONITORING REQUIREMENTS AT THE HOST LEVEL

The following are requirements for the Security Monitoring Subsystem at a host computer system in a network.

a. Obtain via a data link from the host operating system all unsuccessful attempts to access the host. Process each unsuccessful attempt by checking to see if other attempts have occurred from the same source or source area in a relatively short period of time. Record each unsuccessful attempt in the security log.

b. Obtain from the host operating system a record of each person allowed access to the host. Process each record by updating the logical configuration of the host and make a record of the access on the security log.

c. Obtain from the host a record of each action requested by a user. Process each action by checking it against a profile of legal actions and make a record of each action in the security log.

d. Communicate to the Network Security Monitoring Subsystem at the Network Control Center all actions by a user that involve the resources of another host.

e. Make a record in the security log of all information that is either added, changed, or deleted from files that require protection.

f. Obtain from the host a record of each logical interconnection established to the host, process this interconnection by checking it against a list of legal interconnections, update the current logical configuration, and make a record of the interconnection in the security log.

g. Obtain from the host a record of each hardware or software failure, process the failure by determining a level of seriousness, and make a record of the error in the security log.

h. Periodically initiate security verification programs at the host. Obtain, process, and record the results.

i. Periodically summarize events recorded on the security log and print the summaries for review by security personnel.

j. When requested by the Network Control Center, increase information flow to the Network Security Monitoring Subsystem.

3.2. SECURITY MONITORING REQUIREMENTS AT THE NETWORK LEVEL

The following are requirements for the Security Monitoring Subsystem at the Network Control Center.

a. Accept, process, and record all communications from the Host Security Monitoring Subsystems at all nodes in the network.

b. Maintain and record all changes in the current physical and logical configuration of the network down to the host level but including all logical interconnections between hosts.

c. Provide a capability for monitoring at the host level for nodes with limited monitoring capabilities, such as a TIP, and as a backup for the host monitoring subsystem.

3.3. DESIGN REQUIREMENTS FOR A SECURITY MONITORING SYSTEM

The following are requirements for the design of a monitoring system.

a. Security Monitoring should take place in an environment that is as remote from the normal operations of the network as possible with a data path as the only interface to the monitoring systems.

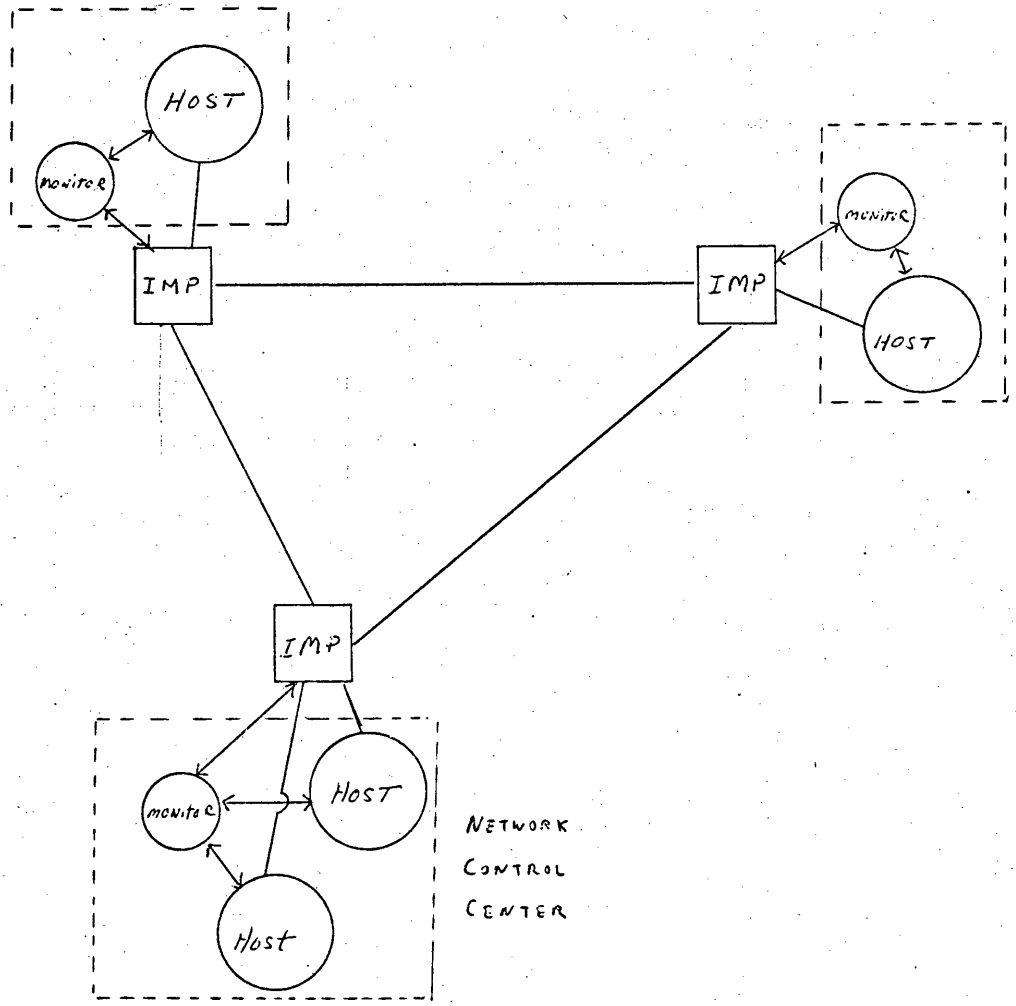
b. Since the volume of information to the monitoring system will vary, there must be a management scheme for sorting and queueing this information so that the more important information is processed first and no information is lost.

c. Since the information processing requires historical data from the security log and profiles from a data base, there must be an information retrieval system to answer querries and to update profiles.

d. Information in the security log along with current configuration information should be available for display to security personnel.

e. When information is processed and an abnormal situation is determined, there should be various methods to warn security personnel of the situation. These methods should coincide with a priority level in which a timely reaction is required.

FIGURE 1



REFERENCES

A. Security Controls for Computer Systems, by Willis H. Ware, Rand Corporation.

B. Computer Security Management, by Dennis Van Jassel, Prentice-Hall, Inc.

C. COINS Network Monitoring System Conceptual Design, Computer Sciences Corporation, Contract BOA DAAB 03-74-A-004.

D. An Investigation into the Application of Minicomputers to Computer System Auditing, by Robert A. Mikelskas, Mitre Corporation, M74-113.

E. Data Sentinel Computer Security System, Basic Computing Arts, Inc.

STAT